

Hackeado por Godzilla

Hace pocos días, ha aparecido un “nuevo” virus en la escena, se trata de un virus bastante inofensivo, que cambia el título del navegador Internet Explorer poniéndole “hacked by godzilla”, resalto la palabra nuevo, por que recién aparece por estos lares, pero este gusano apareció en la escena mundial en el año 2006 y su nombre es **VBS/Solow.A**

Este gusano se difunde rápidamente utilizando las llamadas memorias USB, llaves USB o discos USB.

Si te has percatado que cuando usas Internet aparece “hacked by godzilla”, entonces te será útil la siguiente información para que puedas eliminar ese virus de tu ordenador, de paso que aprendes una que otra cosilla.

Primero quiero comentar que hay virus que colocan una determinada página Web de inicio (por lo general pornográfica) y la congelan, esto quiere decir que no puedes cambiar la página de inicio (que muchos la tenemos apuntando al Google), otros virus, impiden el acceso al Task Manager o administrador de tareas, esto para evitar que puedas detener un proceso, ojo que si el virus está bien hecho, así tengas disponible el Task Manager, no podrás detenerlo así por así, hay una técnica que explicaré en otra columna... Otros virus evitan el acceso al editor del registro (regedit), para evitar que en forma manual puedas reparar los estropicios causados por el virus, otros virus algo más agresivos, impiden que ejecutes comandos (clic en Inicio, clic en ejecutar) y también impiden el acceso a la línea de comandos (esa ventana del D.O.S., que aparece utilizando CMD).

Cuando una máquina está infectada, en la mayoría de veces prefiero formatearla, para mí es más fácil, pero resulta que hay clientes que tienen información desperdigada por todo el disco duro y salvarla es algo complicado o le toma mucho tiempo, en otros casos (como el de mi PC), tengo instaladas un montón de herramientas que utilizo para mi trabajo y créame... reinstalar todo, me toma al menos 3 días, así que en esos casos trato de eliminar los virus sin formatear la máquina.

Formatear la máquina, significa borrar absolutamente TODO el contenido de un disco duro, así que ojo ten cuidado de salvar tu documentación antes de pedir que te formateen el disco duro.

A mis clientes, siempre les aconsejo que guarden todo en el disco D:, cosa que cuando se formatea el disco del sistema, que por lo general es C:, no pierdes nada, muchas personas por flojera graban en la primera opción que les presenta el Excel o el Word, es decir guardan sus trabajos en “mis documentos” que está en C: y es un candidato a perderse en caso de formatear el **HD** (léase disco duro), cuando con un par de clic puedes crear tu carpeta en el disco D: y de paso que tienes tus documentos ordenados.

Bueno volviendo al tema de las restricciones que ponen los virus y debido a la solicitud de varios lectores y personas que siguen mi programa de TV en un canal local, he creado una herramienta a la que he bautizado como **xTools**, esta herramienta desbloquea todas las restricciones señaladas líneas arriba, lo que te permite tratar de eliminar los virus sin tener que formatear la máquina, siguiendo mi costumbre, este

programa mide tan solo 0.03 Mb., es gratuito y no contiene publicidad (toda una maravilla), puedes descargarlo desde **www.hacha.org**

Bueno ahora que estas premunido de esa herramienta y de haber liberado todo, debes hacer lo siguiente: abres el TaskManager, pulsando las teclas **Ctrl.+Alt+Suprimir**, como este gusano fue escrito en Visual Basic Script, en la lista que va a aparecer, ubicas **WSCRIPT** le das clic sobre el nombre y haces clic en el botón “Finalizar tarea”, ojo que puede haber corriendo mas de una vez el wsript, debes detener todas.

A continuación abres el explorador de Windows (Inicio – todos los programas – accesorios – explorador de Windows), en la parte superior en el menú, haces clic en **Herramientas y Opciones de carpeta**, luego clic en la pestaña **ver**, ahí, en la sección “**Configuración avanzada**”, verificas que este marcada la opción “**Mostrar todos los archivos y carpetas ocultos**”, mas abajo desmarcas (al final debes volverlos a marcar) las opciones “**Ocultar las extensiones...**” y la mas importante, debes desmarcar también “**Ocultar archivos protegidos del sistema...**”, al hacer click allí, aparecerá una advertencia, haces clic en el botón **SI**.

Ahora te vas a la carpeta **C:\windows**, ubica y elimina el archivo **MS32DLL.dll.vbs**, luego te vas a **C:\windows\system32** y haces lo mismo, al final, debes ir a la raíz de todos tus discos duros, incluso de tu USB, allí ubicas y eliminas los archivos **autorun.inf** y **MS32DLL.dll.vbs**, ahora abres el editor del registro, para ello, haces clic en el botón Inicio – ejecutar – escribes regedit y pulsas Enter, te desplazas a la siguiente llave: **hkey_local_machine – Software – Microsoft – Windows – CurrentVersion – Run**

En la parte derecha ubicas la entrada que dice: “**MS32DLL**”, haces clic con el botón derecho sobre el nombre y haces clic sobre “Eliminar”, aceptas la confirmación y reinicias tu PC, listo ya eliminaste al gusano y ya no estaras “hackeado” por Godzilla...

Leonardo Donaire Perales

“Dr. Software”

www.hacha.org